UNITED STATES DISTRICT COURT

for the

EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of

Case Number: 13-m-245

A Compaq Presario Desktop computer, Serial Number MXK4150QXR. This device is currently located at the FBI Milwaukee Headquarters Office, 330 E. Kilbourn Avenue, Milwaukee, WI 53202. See Attachment A.

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

I, Jill Dring, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

A Compaq Presario Desktop computer, Serial Number MXK4150QXR. This device is currently located at the FBI Milwaukee Headquarters Office, 330 E. Kilbourn Avenue, Milwaukee, WI 53202. See Attachment A.

located in the Eastern District of Wisconsin there is now concealed: **Please see Attachment B, which is hereby incorporated by reference.**

The basis for the search warrant under Fed. R. Crim. P. 41(c) is which is (check one or more):

- ✓ evidence of a crime;
- ❑ contraband, fruits of a crime, or other items illegally possessed;
- ❑ property designed for use, intended for use, or used in committing a crime;
- ❑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Title 18, United States Code, Section 1951(a); Title 18, United States Code, Section 924(c).

The application is based on these facts:

✓ Continued on the attached sheet, which is incorporated by reference.

❑ Delayed notice of ____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Name and Title: Jill Dring, Special Agent FBI

Sworn to before me, and signed in my presence.

Date June 21, 2013

City and state: Milwaukee, Wisconsin

Judge's signature

THE HONORABLE PATRICIA J. GORENCE

United States Magistrate Judge

Name & Title of Judicial Officer

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Jill Dring, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been employed by the FBI since March 2013. I am currently assigned to the Milwaukee Field Office. In this position, I have been involved in the investigation of, among other things, armed robberies in violation of federal law.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Compaq Presario Desktop computer, Serial Number MXK4150QXR, hereinafter the "Device." The Device is currently located at the FBI Milwaukee Headquarters Office located at 330 E. Kilbourn Avenue, Milwaukee, WI 53202. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

5. This request for authorization to search the above-described Device stems from an investigation into the robbery of Wal-Mart Market, 3850 North 124th Street, Wauwatosa, on

March 22, 2013, at around 2:49 a.m. At that time, two masked individuals entered the Wal-Mart; one carried a pistol and the other carried a rifle. Witness statements and surveillance footage from Wal-Mart reveal that the robbery suspects arrived and departed from the Wal-Mart in a white Buick sedan. During the robbery, the robbers rounded up several Wal-Mart employees including the manager, forced the manager to disable an alarm and open the cash office, collected U.S. currency from the cash office, and ran out of the building.

6. As part of the investigation into the robbery, law enforcement interviewed all of the Wal-Mart employees, and reviewed surveillance video footage taken from inside and outside of the Wal-Mart building at the time of the robbery.

7. During the investigation of the robbery on March 22, 2013, the date of the robbery, a confidential informant (C.I.) contacted law enforcement with information regarding the robbery. In particular, C.I. provided information to law enforcement indicating that C.I. knew the individuals involved in the robbery.

8. Based on the information developed during the investigation, including information provided by C.I., law enforcement came to believe that several individuals may have been involved in the robbery. These individuals included Michael Robertson, Kovan Nash, and Richard Mayberry. The information provided by C.I. was detailed and corroborated by law enforcement.

9. Among other things, C.I. informed law enforcement that Robertson, Nash, and Mayberry planned the robbery on the evening of March 21, 2013, at Mayberry's residence located at 3041 North 35th Street.

10. On the evening of March 22, 2013, law enforcement located Robertson, Nash, and Mayberry. These individuals were arrested in connection with the robbery and taken into custody.

11. During a post-arrest interview with law enforcement on March 22, 2013, Robertson admitted to being involved in the robbery. He has been charged by indictment in Case No. 13-CR-56 (E.D. Wis.) with Interference with Commerce by Robbery, in violation of 18 U.S.C. § 1951(a); and Using, Possessing, or Carrying a Firearm in Connection with a Crime of Violence, in violation of 18 U.S.C. § 924(c).

12. During the post-arrest interview, Robertson identified Kovan Nash and Richard Mayberry as individuals with whom he planned and executed the armed robbery. According to Robertson, he, Nash, and Mayberry met at Mayberry's residence shortly before the robbery. Robertson stated that he and Nash were the ones who entered and robbed the Wal-Mart. After the robbery, Robertson and Nash drove away from Wal-Mart in the white Buick sedan and met up with Mayberry, who was driving a green SUV, a short distance from the Wal-Mart. They then switched vehicles, with Mayberry driving away in the white Buick Sedan, in an effort to confuse law enforcement.

13. Milwaukee Police Department records show that Mayberry was pulled over by Milwaukee Police Officers while driving a white Buick sedan at around 3:15 a.m. on March 22, 2013, which is within a half-hour of the robbery.

14. When interviewed by law enforcement on March 22, 2013, Mayberry denied involvement in the Wal-Mart robbery. Mayberry was asked for his consent for law enforcement to search his residence located at 3041 North 35th Street. Mayberry declined to provide consent,

and informed law enforcement that the property was a rental property. He went on to say that the property was vacant but that a former tenant may have left property there.

15. On March 25, 2013, Wauwatosa Police Department officers executed a search warrant at Mayberry's residence, 3041 North 35th Street. During the officers recovered the Device. In addition, officers recovered the following:

a. Handwritten map of the inside of the Wal-Mart Market.

b. Various pieces of identifying mail/paperwork for 3041 North 35th Street.

c. Two Wisconsin Drivers licenses in the name of Richard Mayberry

d. Thirty-eight CCI brand .22 cal LR rim fire bullets

16. Based on my experience and training, I know that subjects involved in crimes often perform research on computers regarding the targets of their crimes and materials and other locations and items that may be used to facilitate or cover-up their crimes. In addition, subjects involved in crimes often use computers and other electronic devices to communicate with accomplices using email.

17. Wauwatosa Police transferred the Device to the FBI on June 13, 2013. The Device is currently in the lawful possession of the FBI in Milwaukee, Wisconsin. For the reasons stated above, the FBI likely already has the necessary authority to examine the Device. However, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

18. The Device is currently in storage at the FBI's office located at 330 Kilbourn Street in Milwaukee, Wisconsin. In my training and experience, I know and believe that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in

substantially the same state as they were when the Device first came into the possession of law enforcement.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

20. Based on my training and experience, consulting other members of law enforcement familiar with this type of technology, I know that the Device likely has capabilities that allow it to serve as a storage medium and is capable of accessing the Internet and sending and receiving e-mail.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system

configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property to be searched is a Compaq Presario Desktop computer, Serial Number MXK4150QXR, hereinafter the "Device." The Device is currently located at the FBI Milwaukee Headquarters Office located at 330 E. Kilbourn Avenue, Milwaukee, WI 53202. This warrant authorizes the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 1951(a) and 18 U.S.C. 924(c) and involve Richard Mayberry and/or his associates, including Michael Robertson and Kovan Nash, since January 1, 2013, including:

   a. Recent Email history and frequency to and from individuals suspected to be involved in the March 22, 2013 robbery of Wal-Mart Market;

   b. Information relating to efforts to obtain transportation, firearms, ammunition, clothing, and related items used or associated with the March 22, 2013 robbery of Wal-Mart Market;

   c. Information relating to plans, addresses, or locations, of other potential robbery targets;

   d. Information relating to browsing history, or use of the internet to develop the plan to rob the Wal-Mart Market;

   e. Information related to the current location of the firearms used in the robbery, U.S. currency obtained during the robbery, and clothing worn during the robbery;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, saved usernames and passwords, documents, and browsing history;

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.